PHR identifiable health information of 500 or more residents of such State or jurisdiction is, or is reasonably believed to have been, acquired during such breach.

(c) *Notice to FTC.* Vendors of personal health records and PHR related entities shall provide notice to the Federal Trade Commission following the discovery of a breach of security. If the breach involves the unsecured PHR identifiable health information of 500 or more individuals, then such notice shall be provided as soon as possible and in no case later than ten business days following the date of discovery of the breach. If the breach involves the unsecured PHR identifiable health information of fewer than 500 individuals, the vendor of personal health records or PHR related entity may maintain a log of any such breach, and submit such a log annually to the Federal Trade Commission no later than 60 calendar days following the end of the calendar year, documenting breaches from the preceding calendar year. All notices pursuant to this paragraph shall be provided according to instructions at the Federal Trade Commission's Web site.

§ 318.6 Content of notice.

Regardless of the method by which notice is provided to individuals under § 318.5 of this part, notice of a breach of security shall be in plain language and include, to the extent possible, the following:

(a) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

(b) A description of the types of unsecured PHR identifiable health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code);

(c) Steps individuals should take to protect themselves from potential harm resulting from the breach;

(d) A brief description of what the entity that suffered the breach is doing to investigate the breach, to mitigate harm, and to protect against any further breaches; and

(e) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an email address, Web site, or postal address.

§ 318.7 Enforcement.

A violation of this part shall be treated as an unfair or deceptive act or practice in violation of a regulation under § 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices.

§ 318.8 Effective date.

This part shall apply to breaches of security that are discovered on or after September 24, 2009.

§ 318.9 Sunset.

If new legislation is enacted establishing requirements for notification in the case of a breach of security that apply to entities covered by this part, the provisions of this part shall not apply to breaches of security discovered on or after the effective date of regulations implementing such legislation.

PART 320—DISCLOSURE REQUIREMENTS FOR DEPOSITORY INSTITUTIONS LACKING FEDERAL DEPOSIT INSURANCE

AUTHORITY: 12 U.S.C. 1831t; 15 U.S.C. 41 *et seq*

SOURCE: 75 FR 31687, June 4, 2010, unless otherwise noted.

§ 320.1 Scope.

This part applies to all depository institutions lacking federal deposit insurance. It requires the disclosure of certain insurance-related information in periodic statements, account records, locations where deposits are normally received, and advertising. This part also requires such depository